

FIG. 1A

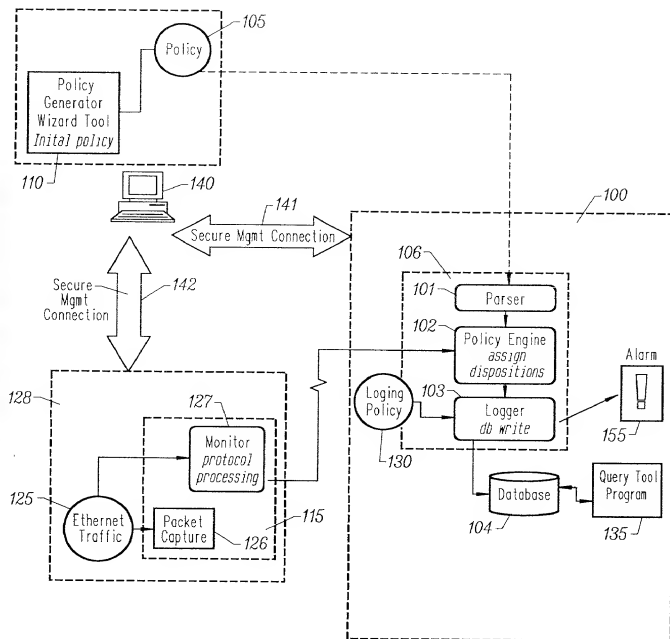


FIG. 1B

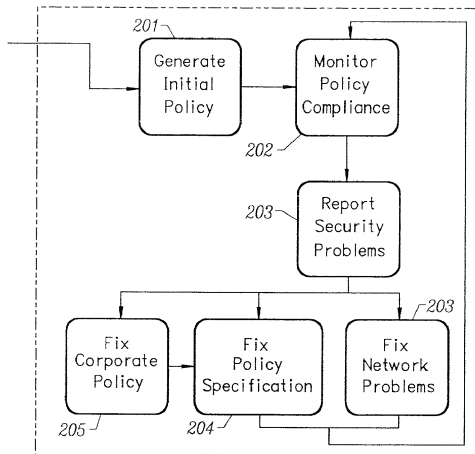


FIG. 2

301

K Policy Generator

File Help

☐ ☐ ☐ ☐

| Community | | Policy Domains | Rules | Service | | |
|---------------|------------|----------------|--|---------|--|--|
| Name | Includes | Excludes | Description | | | |
| Inside_Nodes | 10.0.0.0/8 | | The Hosts in out Intranet <input type="checkbox"/> | | | |
| Outside_Nodes | | Inside_Nodes | All hosts in the Intranet <input type="checkbox"/> | | | |

☐ New

FIG. 3

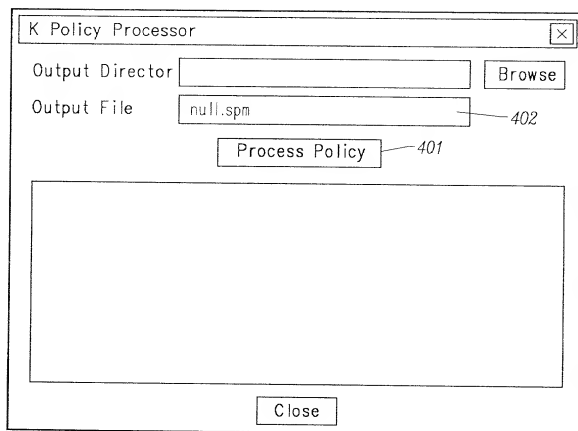


FIG. 4A

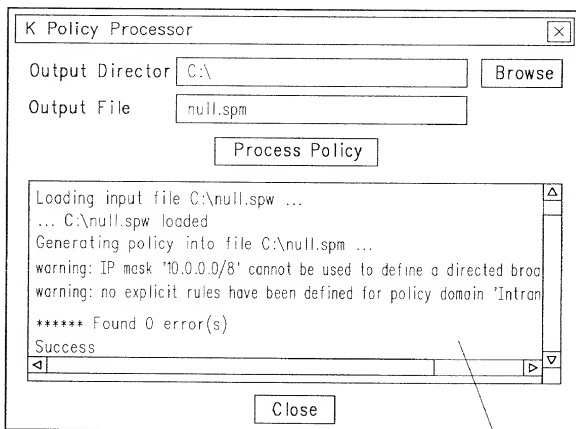


FIG. 4B

SPM: Argument Selector Dialog

Monitor configuration

Input dump file: C:\vqs.dmp 507 Browse

Policy: C:\null.spm 502 Browse

Monitoring Point: INTRANET_MONITOR 503
(comma separated)

Monitor Logging Options

Execution Run Comment:

ODBC name: sybase 504

DB Username: policy 505

DB Password: ***** 506 ☒ Save Password [insecure]

Output Options

☐ Output to console:

☒ Output to file: C:\output.txt Browse

Run Exit Advanced Help

Progress

nPkts 100% 0%

FIG. 5

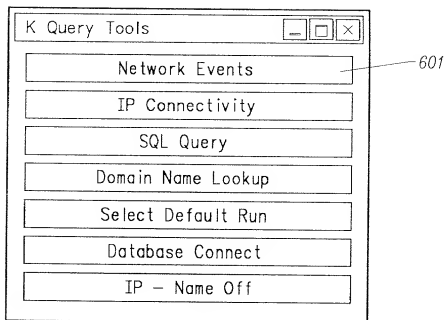


FIG. 6

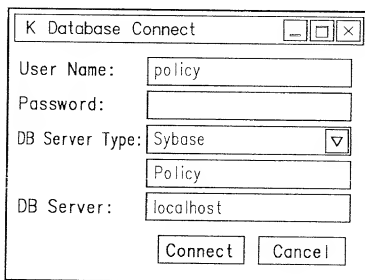


FIG. 7

| | | | |
|-----------------------|--|--|--|
| K Rule View | | X | |
| Execution Run: | | 1999-10-01 14:30:20.0 C:\ bmp | |
| Final Rule Name: | | <Any Rule> | |
| Disposition Name: | | <Any Disposition> | |
| Disposition Codes: | | <input type="checkbox"/> Access Denied <input type="checkbox"/> Auth Violation <input type="checkbox"/> Security Attack <input type="checkbox"/> Security DOS <input type="checkbox"/> Policy Error <input type="checkbox"/> OK | |
| Disposition Severity: | | <input type="checkbox"/> Critical <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Monitor <input type="checkbox"/> Warning <input type="checkbox"/> Information <input type="checkbox"/> <none> | |
| | | Query | |
| | | | |
| Rows | | | |
| | | Done Edit SQL Copy Row Copy Deep | |

FIG. 8

K Rule View

Execution Run: 1999-10-01 14:30:20.0 C:\bnp

Final Rule Name: <Any Rule>

Disposition Name: <Any Disposition>

Disposition Codes: ☐ Access Denied ☐ Auth Violation ☐ Security Attack ☐ Security DOS ☐ Policy Error ☐ OK

Disposition Severity: ☐ Critical ☐ High ☐ Medium ☐ Monitor ☐ Warning ☐ Information ☐ <none>

Query

| Rule Name | Disposition Name | Initiator IP | Init Name | Target IP | Targ Name | Targ Service |
|------------------------|-------------------------|--------------|---------------------|----------------|--------------------|--------------|
| Udp_Deny | Udp_Access_Denied | 10.5.63.143 | vg-143.security.com | 10.5.63.6 | dude.security.com | domain |
| Http_Deny | Http_Access_Denied | 10.5.63.143 | vg-143.security.com | 208.178.27.198 | | http |
| Http_Deny | Http_Access_Denied | 10.5.63.143 | vg-143.security.com | 208.178.27.201 | | http |
| Http_Deny | Http_Access_Denied | 10.5.63.143 | vg-143.security.com | 208.178.27.198 | | http |
| Udp_Deny | Udp_Access_Denied | 10.5.63.143 | vg-143.security.com | 10.5.63.6 | dude.security.com | domain |
| Udp_Deny | Udp_Access_Denied | 10.5.63.143 | vg-143.security.com | 10.5.63.6 | dude.security.com | domain |
| Http_Deny | Http_Access_Denied | 10.5.63.143 | vg-143.security.com | 204.71.200.68 | www3.yahoo.com | http |
| Udp_Deny | Udp_Access_Denied | 10.5.63.143 | vg-143.security.com | 10.5.63.6 | dude.security.com | domain |
| Http_Deny | Http_Access_Denied | 10.5.63.143 | vg-143.security.com | 10.5.63.97 | kable.security.com | http |
| Tcp_Missed_Connections | Warn_Missed_Top_Connect | 10.5.63.143 | vg-143.security.com | 10.5.63.24 | fred.security.com | netbios-ssn |

Rows 10

Done Edit SQL Copy Row Copy Deep

FIG. 9

| | | | | | |
|---|--|--|--|---|--|
| K Policy Generator | | | | <input type="button" value="X"/> <input type="button" value="□"/> <input type="button" value="□"/> | |
| File Help | | | | | |
| <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> | | | | | |
| Community | | Policy Domains | | Rules Service | |
| Select Policy Domain Policy Domain: <input type="text" value="Intranet"/> | | | | | |
| Identify New or Existing Rule in Intranet | | | | | |
| Rule Name: | | <input type="text" value="Internal_Dns"/> <input type="button" value="New"/> <input type="button" value="X Delete"/> | | | |
| Add Elements to Internal_Dns | | | | | |
| Description: | | | | | |
| <div> <div> <div>Initiators:</div> <div> <div> <input type="button" value="Add Selected"/> </div> <div> <div>== Intranet ==</div> <div>Inside_Nodes</div> <div>... Firewall ...</div> <div>Outside_Nodes</div> </div> </div> <div> <div>Services:</div> <div> <div> <input type="button" value="Add Selected"/> </div> <div> <div>AUTH</div> <div>BOOTP_CLIENT</div> <div>BOOTP_SERVER</div> <div>DNS</div> <div>FINGER</div> </div> </div> </div> <div> <div>Targets:</div> <div> <div> <input type="button" value="Add Selected"/> </div> <div> <div>== Intranet ==</div> <div>Inside_Nodes</div> <div>... Firewall ...</div> <div>Outside_Nodes</div> </div> </div> </div> </div> </div> | | | | | |
| <div>Set</div> | | | | | |
| Rule Contents for Internet* Dns | | | | | |
| Initiators: | | <input type="button" value="Add Selected"/> | | <div> <div>Services:</div> <div> <div> <input type="button" value="Add Selected"/> </div> <div> <div><Any></div> </div> </div> </div> | |
| <div> <div>Targets:</div> <div> <div> <input type="button" value="Add Selected"/> </div> <div> <div><Any></div> </div> </div> </div> | | | | | |

| | | | | | |
|--|----------------|--|------------------------------------|--|--|
| K Policy Generator | | | | <input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="X"/> | |
| File Help | | | | | |
| <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> | | | | | |
| Community | Policy Domains | Rules | Service | | |
| Select Policy Domain | | | Policy Domain: | Intranet ▾ | |
| Identify New or Existing Rule in Intranet | | | Rule Name: | Internal_Dns ▾ | <input type="checkbox"/> New <input type="button" value="X"/> Delete |
| Add Elements to Internal_Dns | | | Description: | | |
| Allow DNS to be served from any internal host | | | <input type="button" value="Set"/> | | |
| Initiators: | | Services: | | Targets: | |
| <input type="checkbox"/> Intranet <input checked="" type="checkbox"/> Inside_Nodes ... Firewall ... Outside_Nodes | | AUTH BOOTP_CLIENT BOOTP_SERVER DNS FTINGER | | <input type="checkbox"/> Intranet <input checked="" type="checkbox"/> Inside_Nodes ... Firewall ... Outside_Nodes | |
| <input type="button" value="Add Selected"/> | | <input type="button" value="Add Selected"/> | | <input type="button" value="Add Selected"/> | |
| Rule Contents for Internet* Dns | | | | | |
| Initiators: | | Services: | | Targets: | |
| <input type="checkbox"/> Inside_Nodes | | DNS | | <input type="checkbox"/> Inside_Nodes | |
| <input type="button" value="Add Selected"/> | | <input type="button" value="Add Selected"/> | | <input type="button" value="Add Selected"/> | |

K Policy Generator

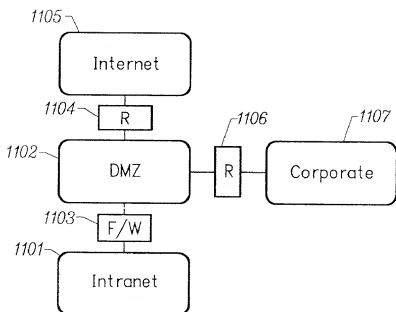
File Help

☐ ☐ ☐ ☐

| Community | Policy Domains | Rules | Service |
|---------------|----------------|--------------|--|
| Name | Includes | Excludes | Description |
| Inside_Nodes | 10.0.0.0/8 | | The Hosts in out Intranet <input type="checkbox"/> |
| Outside_Nodes | | Inside_Nodes | All hosts in the Intranet <input type="checkbox"/> |

☐ New

FIG. 10C

*FIG. 11*

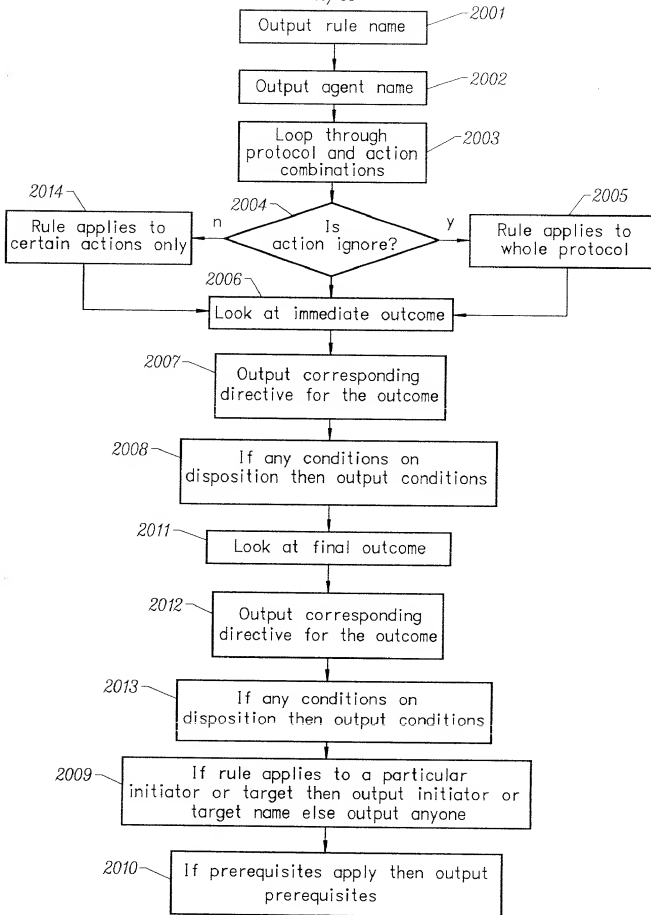


FIG. 12

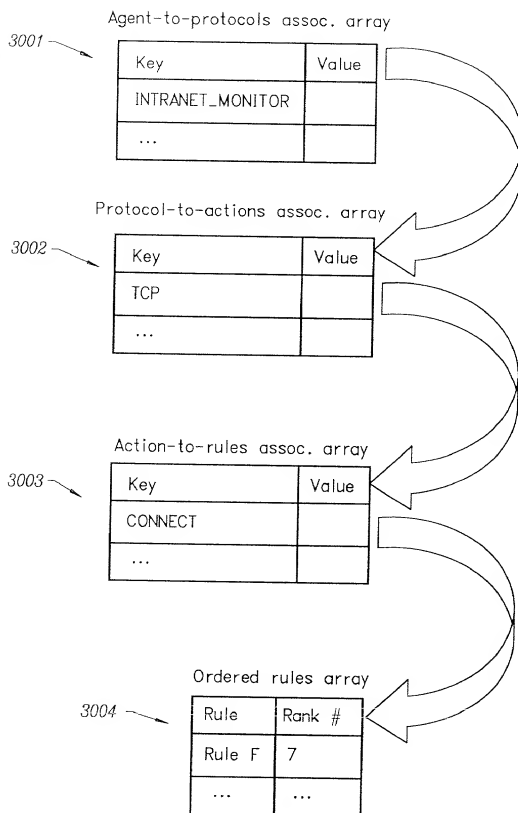


FIG. 13

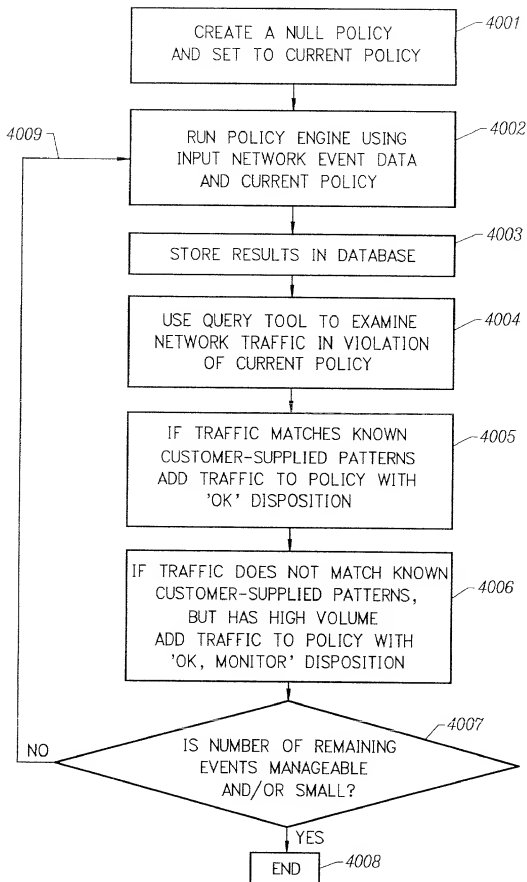


FIG. 14

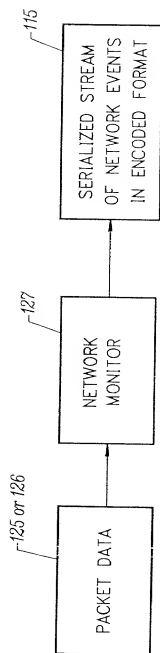


FIG. 15

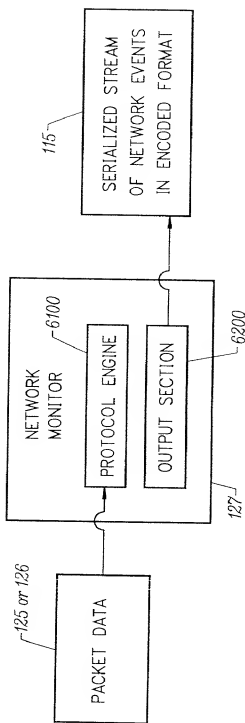


FIG. 16

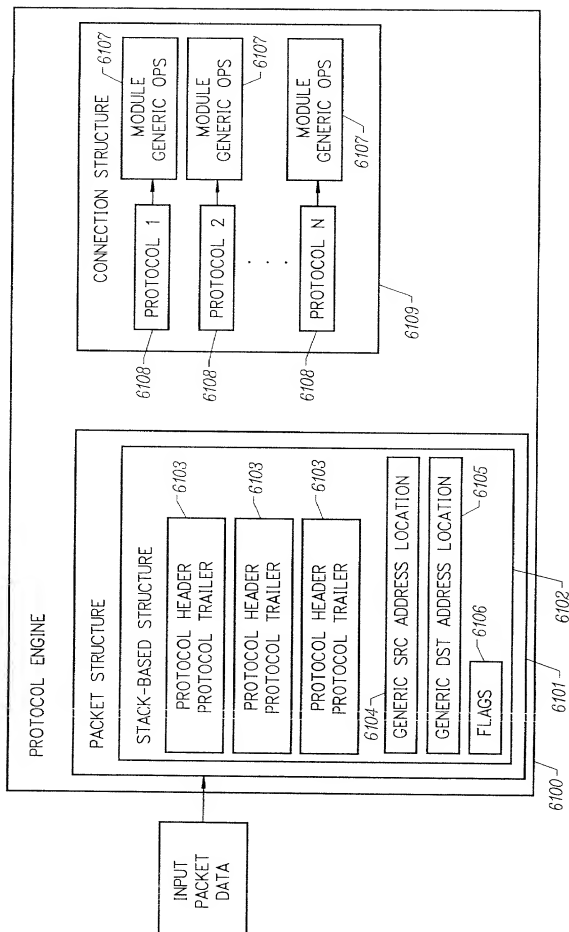


FIG. 17

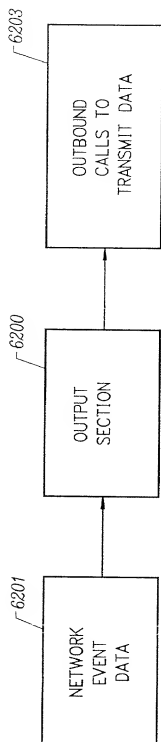


FIG. 18

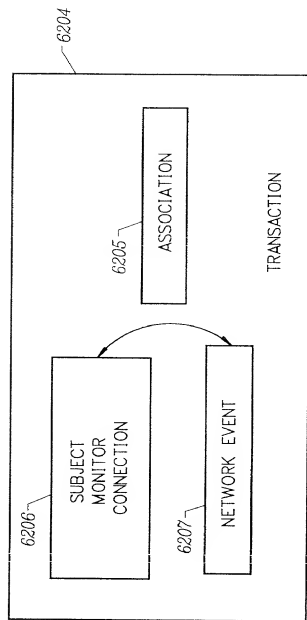
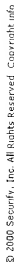


FIG. 19

2000-



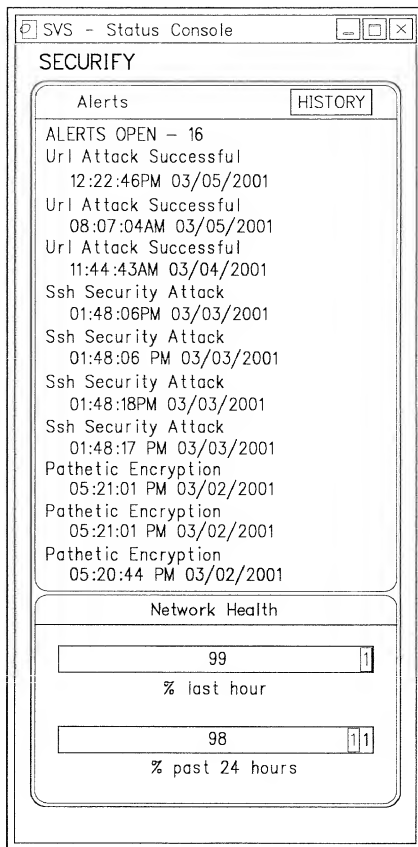


FIG. 21

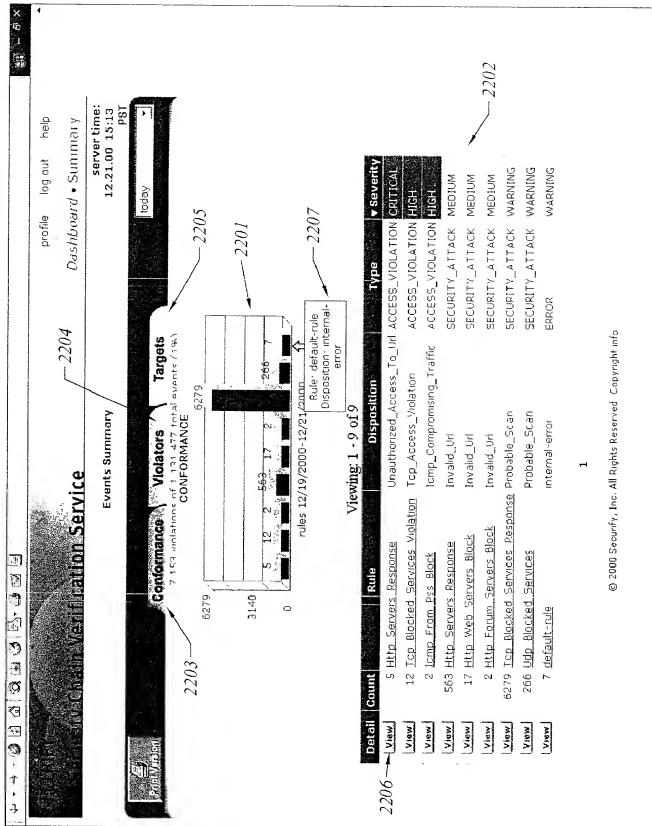
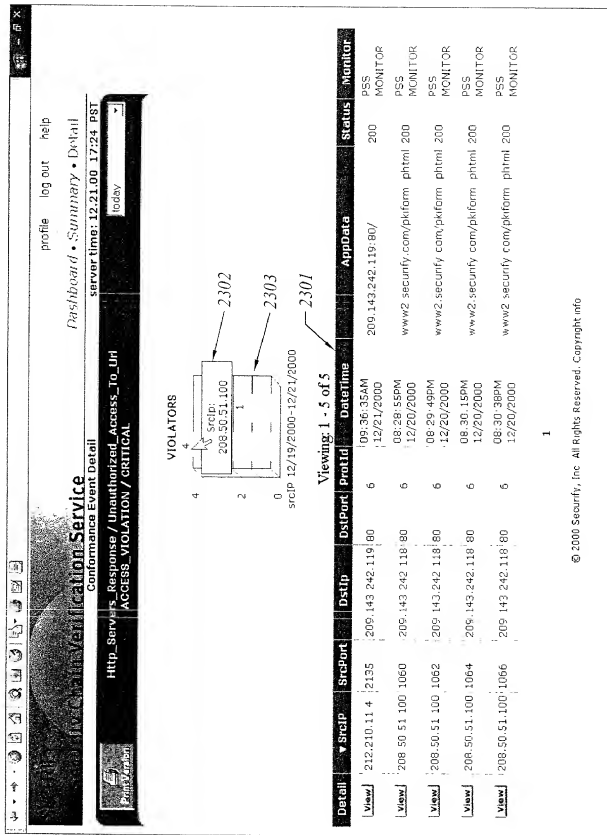


FIG. 22

FIG. 23



City Chalmers Verification Service

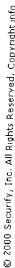


FIG. 25

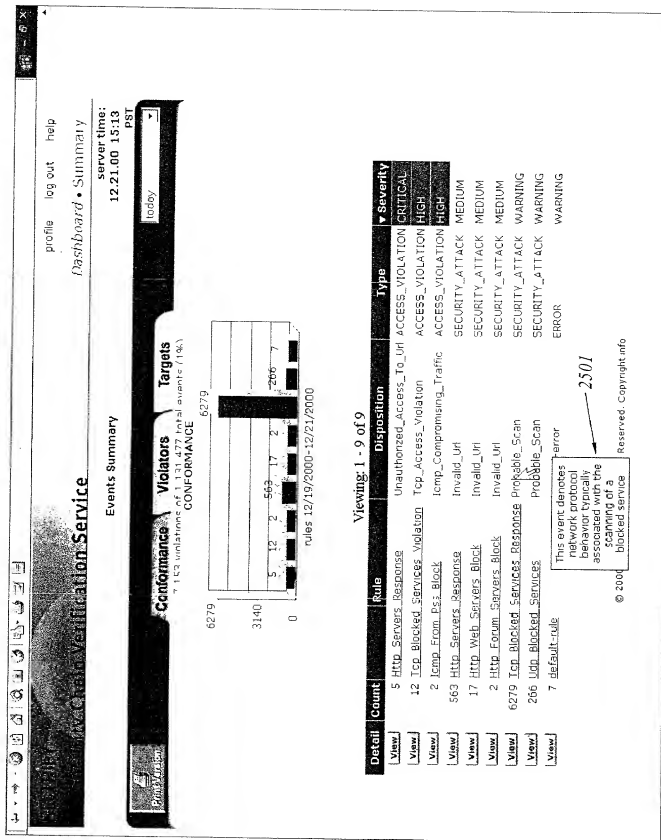


FIG. 26

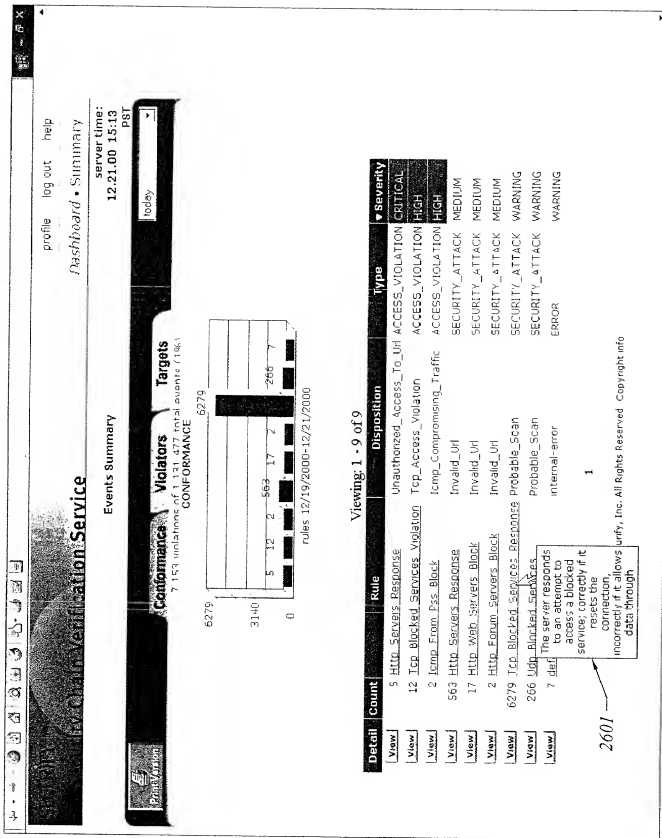
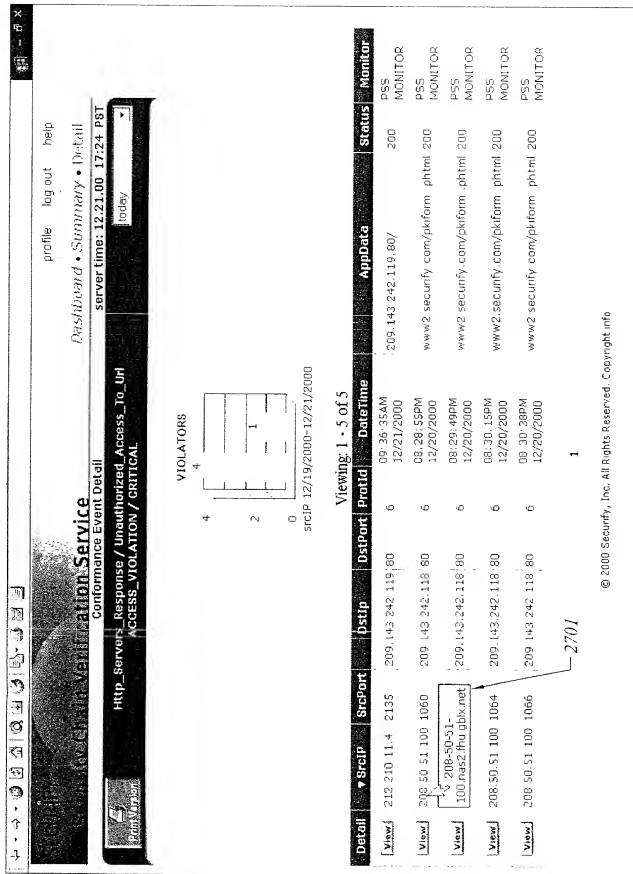


FIG. 27

28/33



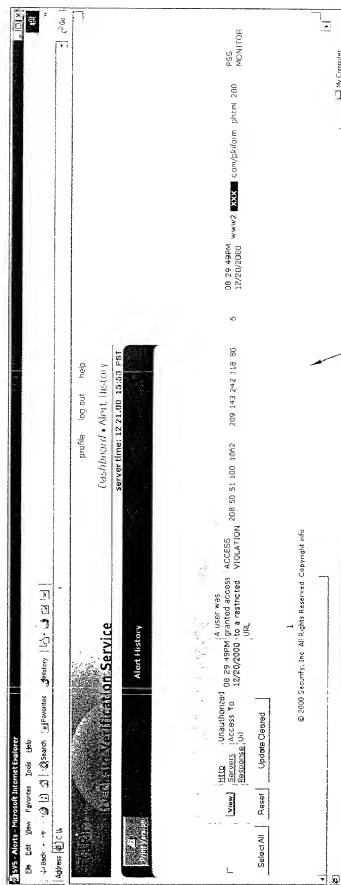


FIG. 28

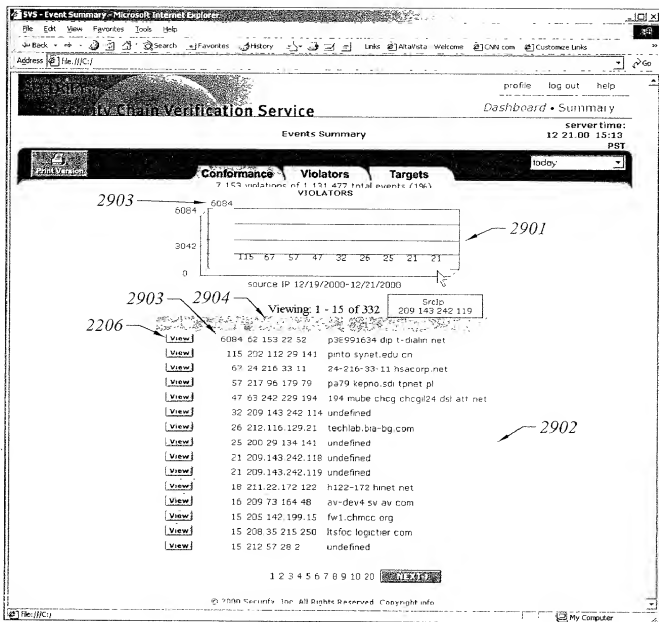


FIG. 29

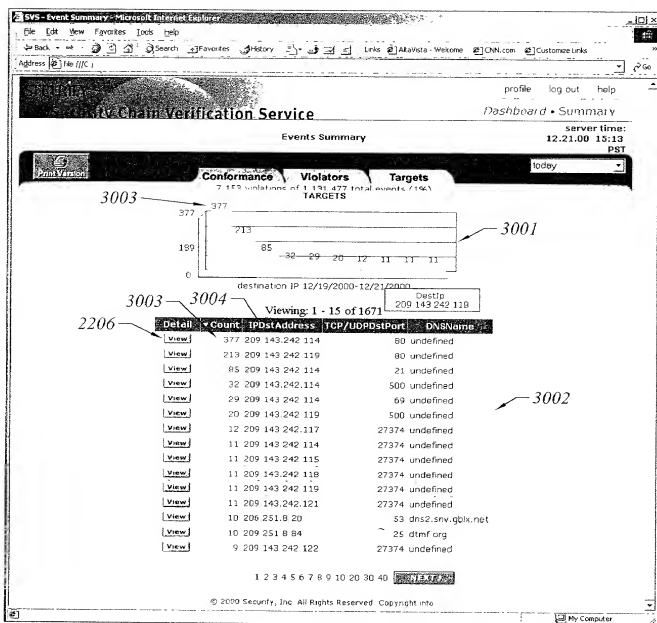


FIG. 30

Address <https://> Go

SECURIFY

Advanced Search

Filter results by One or All of the following:

Protocol

Rule

or

(regular expression in Rule)

Disposition

or

(regular expression in Disposition)

Source IP

Target IP

TargetPort

Monitor(s)

INTRANET_LOCAL_MONITOR
INTRANET_MONITOR
PARTNER_A_MONITOR

© 2000, 2001 Securify, Inc. All Rights Reserved.
Copyright info

FIG. 31

FIG. 32

3201

